PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140304
(43)Date of publication of application : 17.05.2002

(51)Int.Cl. G06F 15/00
G06F 17/60
G10K 15/02
G10L 19/00
H04Q 7/38
H04L 9/32
H04L 12/28

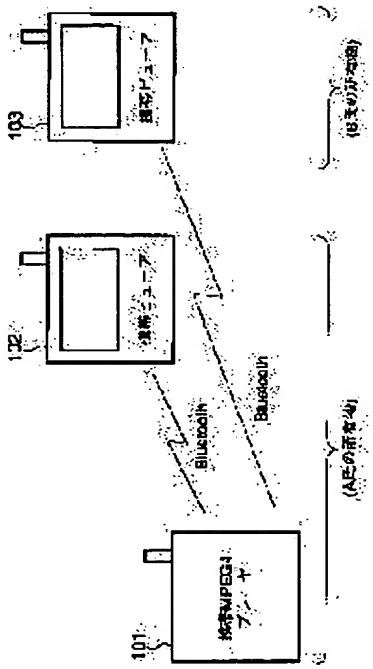
(21)Application number : 2001-028544
(22)Date of filing : 05.02.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : SAITO TAKESHI

(30)Priority
Priority number : 2000252882 Priority date : 23.08.2000 Priority country : JP

(54) RADIO COMMUNICATION SYSTEM, TRANSMITTER, RECEIVER, AND CONTENTS DATA TRANSFER METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a radio communication system which can actualize safe copyright protection even in a radio environment.
SOLUTION: An authenticating and key exchanging procedure of a radio link layer network is carried out between a portable MPEG4 player 101 which sends MPEG4 data whose copyright should be protected and a portable viewer 102 which receives, decodes, and displays the data from the player 101 and when the procedure is successfully followed, an authenticating and key exchanging procedure of DTCP is carried to between the player 101 and viewer 102 by using a cipher communication using a cipher key that the player 101 and viewer 102 shares, and when the authenticating and key exchanging procedure is successfully completed, the data are transferred safely from the player 101 to the viewer 102 by using the cipher communication using the cipher key that the player 101 and viewer 102 shares.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－140304
（P2002－140304A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｃ　５Ｂ０８５
					３３０Ｂ　５Ｊ１０４
					３３０Ｆ　５Ｋ０３３
	17/60	３０２		17/60	３０２Ｅ　５Ｋ０６７
Ｇ１０Ｋ	15/02		Ｇ１０Ｋ	15/02	

審査請求　未請求　請求項の数15　ＯＬ　（全 14 頁）　最終頁に続く

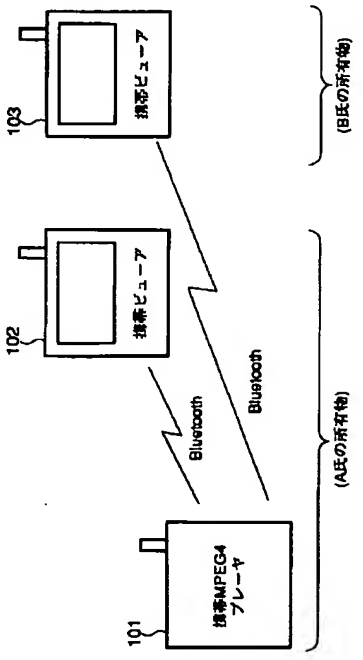
(21)出願番号　特願2001－28544(P2001－28544)
(22)出願日　平成13年２月５日(2001.2.5)
(31)優先権主張番号　特願2000－252882(P2000－252882)
(32)優先日　平成12年８月23日(2000.8.23)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法

(57)【要約】
【課題】　無線環境においても安全な著作権保護を実現可能な無線通信システムを提供すること。
【解決手段】　著作権保護すべきＭＰＥＧ４データを送信する携帯ＭＰＥＧ４プレーヤ１０１と、該プレーヤ１０１から該データを受信し、デコードして表示する携帯ビューア１０２との間で、無線リンクレイヤネットワークの認証・鍵交換手続きを行い、この認証・鍵交換手続きの成功によってプレーヤ１０１とビューア１０２との間で共有された暗号鍵を用いた暗号通信を利用して、プレーヤ１０１とビューア１０２との間で、ＤＴＣＰの認証・鍵交換手続きを行い、この認証・鍵交換手続きの成功によってプレーヤ１０１とビューア１０２との間で共有された暗号鍵を用いた暗号通信を利用して、プレーヤ１０１からビューア１０２へ、安全に該データを転送する。



1

【特許請求の範囲】

【請求項１】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項２】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

2

【請求項３】著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする無線通信システム。

【請求項４】著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。

【請求項５】前記第２の認証手段または前記第２の鍵交換手続き手段は、前記無線リンクレイヤ上における暗号化通信が介在しなかったことを理由として、前記著作権保護のための認証または前記第２の暗号鍵の共有が失敗した場合に、該失敗の旨および該理由を前記受信装置に通知することを特徴とする請求項３または４に記載の送信装置。

【請求項６】前記コンテンツ・データを記憶するための記憶手段を更に備えたことを特徴とする請求項３ないし５のいずれか１項に記載の送信装置。

【請求項７】前記第１の認証手段による前記認証は、自装置に入力されたＰＩＮコードと前記受信装置から通知されたＰＩＮコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項３ないし６のいずれか１項に記載の送信装置。

【請求項８】前記ＰＩＮコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項３ないし７のいずれか１項に記載の送信装置。

【請求項９】著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項１０】著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置との間で著作

権保護のための認証が成功した場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項１１】前記コンテンツ・データを表示するための表示手段を更に備えたことを特徴とする請求項９または１０に記載の受信装置。

【請求項１２】前記第１の認証手段による前記認証は、自装置に入力されたＰＩＮコードと前記送信装置から通知されたＰＩＮコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項９ないし１１のいずれか１項に記載の受信装置。

【請求項１３】前記ＰＩＮコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項９ないし１２のいずれか１項に記載の受信装置。

【請求項１４】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有し、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有し、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【請求項１５】無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有し、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有し、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線を介して著作権保護を必要とするデータの転送を行う無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法に関する。

【０００２】

【従来の技術】近年、デジタルネットワーク技術の発展が急である。携帯電話やインターネットをはじめとしたネットワーク技術の進歩は、とどまる所を知らず、アプリケーションも、単なる音声通話にとどまらず、多彩なものになってきた。例えば、インターネットにおける音楽配信、あるいは携帯電話に対する無線データ網（ｉ－ｍｏｄｅ（登録商標）など）を介した音楽配信等は、その典型的な例といえよう。

【０００３】一方、デジタル家電と呼ばれる新しい分野も注目を集めている。これは、デジタル技術を用いた新しい家電技術であり、特にデジタル放送の開始や、ＭＤ、ＤＶＤ等のデジタルＡＶ技術を駆使した「デジタルＡＶ家電」の分野は、大変大きな成長が見込まれている。

【０００４】これらの分野が融合したと考えられるものが「ネットワーク家電」の分野である。ＩＥＥＥ１３９４等のネットワークを介してデジタルＡＶデータ（ＭＰＥＧ２映像等）をやり取りすることができ、多くのアプリケーションを新たに生み出すことも可能である。

【０００５】このような状況で考慮しなければならないのが、著作権保護の問題である。デジタルデータは、加工や蓄積が容易、劣化が無い、等の利点がある反面、「コピーしやすい」等の特徴があり、本来、何らかの対価を支払って購入すべきデジタルデータ（例えば映画や音楽など）であっても、これを不正にコピーして入手しあるいは譲渡することが可能なわけである。よって、著作権に係るデジタルデータに対する不正行為を未然に防ぐ仕組みを構築することが重要になる。その代表的な例が、ＩＥＥＥ１３９４におけるＤＴＣＰ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔｓ Ｐｒｏｔｅｃｔｉｏｎ）である。これは、ＩＥＥＥ１３９４上のＡＶデータの送信装置と受信装置との間で、認証・鍵交換の手順を行ない、ＡＶデータを暗号化・復号化するための暗号鍵を共有した上で、この暗号鍵によって、ＡＶデータを暗号化した上でＩＥＥＥ１３９４上を転送することで、第三者による盗聴を防止することができる。また、あらかじめ安全性を保証する機器にしか、上記認証・鍵交換（さらに具体的には、証明書／Ｃｅｒｔｉｆｉｃａｔｅの交換）を行なわせないような工夫をすることで、不正な受信装置での不正コピーを未然に防ぐような仕組みが備わっている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記の仕組みはＩＥＥＥ１３９４やＵＳＢなどの有線ネットワークを前提とした仕組みである。すなわち、無線ネットワークを使ったＡＶデータの転送を考えた場合、装置間でＡＶデータを転送することができてしまうため（ケーブルで装置間を接続する必要が無く、単に無線を経由して、送信を指示するだけでＡＶデータを送信して貰うことが可能であるため）、第三者がコンテンツを傍受することが可能になってしまい、不正行為を防止することができない、と言う問題点があった。

【０００７】本発明は、上記事情を考慮してなされたもので、無線環境においても安全な著作権保護を実現可能な無線通信システム、送信装置、受信装置及びコンテンツデータ転送方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システム／コンテンツデータ転送方法において、前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有し、前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有し、前記

無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする。あるいは、前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする。

【０００９】本発明は、著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第１の認証手段と、この第１の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、この第２の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする。あるいは、前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする。

【００１０】本発明は、著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、自装置が前記コンテンツを受信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第１の認証手段と、この第１の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第２の認証手段と、この第２の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信することを特徴とする。あるいは、前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする。

【００１１】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００１２】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００１３】本発明では、著作権保護すべきコンテンツ・データを送信する送信装置と、該送信装置から著作権保護された該コンテンツ・データを受信する受信装置との間で、無線リンクレイヤネットワークに依存した第１の認証・鍵交換手続きを行い、続いて、著作権保護すべきコンテンツ・データに依存した第２の認証・鍵交換手続きの全部または一部を、第１の認証・鍵交換手続きの成功によって前記送信装置と前記受信装置との間で共有された第１の暗号鍵を用いた暗号通信によって行うので、該第１の認証を成功させることのできる正当な送信装置と受信装置との間でのみ、第２の暗号鍵を用いた暗号通信による該コンテンツ・データの転送を行うことができる。

【００１４】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００１５】（第１の実施形態）図１に、本実施形態の無線通信システムの構成例を示す。

【００１６】図１に示されるように、ソース機器となる携帯ＭＰＥＧ４プレーヤ１０１と、これに対するシンク機器となる携帯ビューア１０２とが、ローカルエリア無線ネットワークで接続できる範囲内に位置している（携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２はそれぞれこのローカルエリア無線ネットワークの無線インタフェースを有するものとする）。

【００１７】ここで、図１に示されるように、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２の他に、携帯ビューア１０３（携帯ビューア１０２と同様の基本構成とする）も携帯ＭＰＥＧ４プレーヤ１０１へローカルエリア無線ネットワークで接続できる範囲内に位置している場合を考える。

【００１８】すなわち、これら３つの携帯端末が同一の無線ＬＡＮ（Ｂｌｕｅｔｏｏｔｈの場合は単一ピコネット）内に存在しており、携帯ＭＰＥＧ４プレーヤからＢｌｕｅｔｏｏｔｈ経由でどちらの携帯ビューアに対して

もＭＰＥＧ４映像を転送することができる範囲内に存在しているものとする。そして、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２は同一人物…Ａ氏とする…の携帯物であり（Ａ氏が対にして使用しようとしているものであり）、携帯ビューア１０３はＡ氏とは異なる人物…Ｂ氏とする…の携帯物である（Ａ氏が使用しようとしていないものである）とする。なお、ここでは簡単のために携帯ビューア１０３について考えるが、Ａ氏以外の人物の携帯する携帯ビューアが他に接続範囲内に存在していても携帯ビューア１０３と同様である。

【００１９】また、転送するＭＰＥＧ４映像（ＭＰＥＧ４データ）は、著作権保護をかけた上で転送すべきものである場合を考える。

【００２０】なお、ここでは、ローカルエリア無線ネットワークとしては、Ｂｌｕｅｔｏｏｔｈを仮定して説明する。Ｂｌｕｅｔｏｏｔｈは、低コスト、低消費電力などを特徴とする無線ＬＡＮの一種であり、多くの携帯端末や家電製品などへの搭載が期待されている（例えば、ｈｔｔｐ：／／ｗｗｗ．ｂｌｕｅｔｏｏｔｈ．ｃｏｍにて取得可能に開示されている文書に説明が詳しい）。また、以下で用いるＢＴの表記は、Ｂｌｕｅｔｏｏｔｈを略したものである。

【００２１】以下、図１のような状況において、携帯ＭＰＥＧ４プレーヤ１０１から携帯ビューア１０２に対してのみＭＰＥＧ４映像を転送可能（携帯ビューア１０２においてのみ再生、視聴可能）とするための構成について説明する。

【００２２】図２に、携帯ＭＰＥＧ４プレーヤ１０１の内部構造の一例を示す。

【００２３】図２に示されるように、携帯ＭＰＥＧ４プレーヤ１０１は、Ｂｌｕｅｔｏｏｔｈの物理レイヤ処理を実行するＢｌｕｅｔｏｏｔｈインタフェース（Ｉ／Ｆ）処理部１１、Ｂｌｕｅｔｏｏｔｈのデータリンクレイヤ処理を実行するｂｌｕｅｔｏｏｔｈ通信処理部１２を備えている。

【００２４】Ｂｌｕｅｔｏｏｔｈは、そのスペック内に「Ｂｌｕｅｔｏｏｔｈ　Ｓｅｃｕｒｉｔｙ」なる認証、鍵交換、データ暗号化の方式が規定されている。つまり、Ｂｌｕｅｔｏｏｔｈというリンクレイヤ方式内部に、データ暗号化や、認証・鍵交換の方式が定められている。携帯ＭＰＥＧ４プレーヤ１０１は、この処理部（ＢＴ認証・鍵交換手続き（データのやり取り）を行うためのＢＴ認証・鍵交換処理部１３、ＰＩＮコードを入力するためのＰＩＮコード入力部１４、送信すべきデータを暗号化し、受信したデータを復号化するためのＢＴレイヤ暗号・復号化部１５）を、内部に持っている。Ｂｌｕｅｔｏｏｔｈレベルの認証は、ＰＩＮコードと呼ばれるコード（例えば、数桁の数字やパスワード、あるいは指紋情報などの身体情報、等）の照合によって行われる。

【００２５】この他、携帯ＭＰＥＧ４プレーヤ１０１は、ＭＰＥＧ４ＡＶデータを蓄積しておくＭＰＥＧ４ストレージ１９、これをＢｌｕｅｔｏｏｔｈパケットに変換するパケット化部１８、さらにＭＰＥＧ４のデータを暗号化して転送するための著作権保護レイヤ（アプリケーションレベル）の処理部（ＤＴＣＰ認証・鍵交換手続き（データのやり取り）を行うためのＤＴＣＰ認証・鍵交換部１６、送信すべきデータを暗号化するためのＤＴＣＰ暗号化部１７）を内部に持つ。

【００２６】ここで、ＤＴＣＰとは、Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔｓ Ｐｒｏｔｅｃｔｉｏｎの略で、ＩＥＥＥ１３９４やＵＳＢなどでデファクトスタンダードとなっている著作権保護の方式である。著作権保護が必要なＡＶデータ（例えば、ＡＶデータに著作権保護が必要か否かを示す情報が付加されている）に対して、送信装置と受信装置との間で、認証・鍵交換を行ない、ＡＶデータを暗号化して転送する仕組みが備わっている（例えば、ｈｔｔｐ：／／ｗｗｗ．ｄｔｌａ．ｃｏｍにて取得可能に開示されている文書に説明が詳しい）。

【００２７】図３に、携帯ビューア１０２（１０３）の内部構造の一例を示す。

【００２８】図３に示されるように、携帯ビューア１０２は、Ｂｌｕｅｔｏｏｔｈインタフェース（Ｉ／Ｆ）処理部２１およびｂｌｕｅｔｏｏｔｈ通信処理部２２、Ｂｌｕｅｔｏｏｔｈレベルの認証・鍵交換や暗号化の処理部（ＢＴ認証・鍵交換手続き（データのやり取り）を行うためのＢＴ認証・鍵交換処理部２３、ＰＩＮコードを入力するためのＰＩＮコード入力部２４、送信すべきデータを暗号化し、受信したデータを復号化するためのＢＴレイヤ暗号・復号化部２５）、ＡＶデータ（アプリケーションレベル）の認証・鍵交換や暗号化を行う処理部（ＤＴＣＰ認証・鍵交換手続き（データのやり取り）を行うためのＤＴＣＰ認証・鍵交換部２６、受信したデータを復号化するためのＤＴＣＰ復号化部２７）を備えている。

【００２９】また、携帯ビューア１０２は、Ｂｌｕｅｔｏｏｔｈパケットを ＭＰＥＧ４データにリアセンブリするパケットリアセンブリ部２８、ＭＰＥＧ４データをデコードするＭＰＥＧ４デコーダ２９、ＭＰＥＧ４データを表示するためのディスプレイ３０を備えている。

【００３０】図４に、Ｂｌｕｅｔｏｏｔｈレイヤの認証手順の概要を示す。各々の装置（携帯ＭＰＥＧ４プレーヤ、携帯ビューア）では、ＰＩＮコードが入力される（ステップＳ１）。なお、ＰＩＮコードは、その都度入力する方法や、予め入力して設定しておく方法などがある。両装置は、（ＢＴ認証・鍵交換処理部１３，２３により）Ｂｌｕｅｔｏｏｔｈレイヤの認証手順を行う（ステップＳ２）。両装置間でＰＩＮコードを交換し、それらのＰＩＮコードが一致して認証に成功すれば（ステッ

ブＳ３）、ｂｌｕｅｔｏｏｔｈレイヤの鍵交換手順が行われ、鍵共有に成功する（ステップＳ４）。この後、（ＢＴレイヤ暗号・復号化部１５，２５が）共有したｂｌｕｅｔｏｏｔｈレイヤの鍵を用いるによって、（ＤＴＣＰ認証・鍵交換部１６，２６による）ＤＴＣＰ認証・鍵交換を安全に行うことができる。これによって、ＤＴＣＰの鍵を共有し、ＭＰＥＧ４データの暗号通信が可能になる（ＤＴＣＰ暗号化部１７で暗号化し、ＤＴＣＰ復号化部２７で復号化することが可能になる）。一方、両装置のＰＩＮコードが一致せず認証に失敗すれば（ステップＳ３）、ｂｌｕｅｔｏｏｔｈレイヤの鍵交換手順が行われるが、鍵共有に失敗する（ステップＳ５）。この場合には、ｂｌｕｅｔｏｏｔｈレイヤの鍵が共有されていないので、たとえ（ＤＴＣＰ認証・鍵交換部１６，２６による）ＤＴＣＰ認証・鍵交換が動作しても、（間違ったｂｌｕｅｔｏｏｔｈレイヤの鍵で復号化を行うことになり）、ＤＴＣＰ認証・鍵交換を成功させることができない（ＤＴＣＰの鍵を共有することができない）。さらに、ＤＴＣＰ認証・鍵交換が成功していなければ、たとえ（ＤＴＣＰ暗号化部１７でＤＴＣＰの鍵を用いて）暗号化されたＭＰＥＧ４データを受信しても、（ＤＴＣＰ復号化部２７では正しいＤＴＣＰの鍵を知らないので）その復号化ができない。なお、両装置のＰＩＮコードが一致せず認証に失敗した場合には、ｂｌｕｅｔｏｏｔｈレイヤの鍵交換手順自体を行わないようにしてもよい。

【００３１】なお、本実施形態では、両装置のＰＩＮコードの値の一致をもって認証の成功としているが、その他、一方のＰＩＮコードの値と他方のＰＩＮコードの値とが予め定められた一定の関係（例えば、ユーザ属性情報として住所情報の一部を利用する関係、等）にある場合に、認証の成功とするようにしてもよい（なお、両装置のＰＩＮコードの値が一致するという関係も、一定の関係の一場合である）。

【００３２】ここで、ＰＩＮコードのバリエーションについて説明する。

【００３３】まず、ＰＩＮコードの入力あるいは設定方法として、種々のバリエーションがある。

【００３４】例えば、（１）ユーザがその都度入力する方法、（２）ユーザが予め設定しておく方法、（３）製造者または販売者等が（ユーザが変更できない形で）予め設定しておく方法、（４）上記の（１）～（３）の全部又は一部を併用する方法（例えば、（１）コードと（３）のコードを連結する等）など、種々の方法が考えられる。また、例えば、ユーザが上記の（１）または（２）について適宜選択可能とする方法もある。

【００３５】また、ＰＩＮコードの内容としても、種々のバリエーションがある。

【００３６】（１）または（２）の方法の場合、例えば、ＰＩＮコードをユーザがその都度決定する方法がある。また、例えば、一方の装置…例えば携帯ＭＰＥＧ４プレーヤ…内でランダムにパスワードを発生させ、これを該一方の装置側でＰＩＮコードとして記憶するとともにユーザに呈示し、これを読み取ったユーザが同一のパスワードを他方の装置…例えば携帯ビューア…に入力する方法もある。また、指紋情報、声門情報、あるいは角膜情報等を用いる方法もある（この場合、それら情報を採取する装置が、携帯ＭＰＥＧ４プレーヤや携帯ビューアに内蔵されているか、または携帯ＭＰＥＧ４プレーヤや携帯ビューアに外部接続可能である必要がある）。

【００３７】また、（２）の方法の場合に、携帯ＭＰＥＧ４プレーヤや携帯ビューアに、ユーザ属性情報が登録されているならば、この情報（例えば、ユーザ名、住所、年令、学校名、職業、会社名、部課名、家族名等）に基づいてＰＩＮコードを生成する方法もある（ただし、ＰＩＮコードを生成するもととなる情報は、両装置でＰＩＮコードを同一にするような値…例えば同一の値…にしておく必要がある）。

【００３８】また、（３）の方法の場合に、製造者または販売者等が、製造時または販売時に、１セットの携帯ＭＰＥＧ４プレーヤや携帯ビューアに同一の乱数を設定しておく方法がある。また、販売者が、販売時に、ユーザの指紋情報等を採取して１セットの携帯ＭＰＥＧ４プレーヤや携帯ビューアに設定しておく方法がある。

【００３９】さて、本実施形態の携帯ＭＰＥＧ４プレーヤおよび携帯ビューアは、「正当な対になるプレーヤ／ビューア間では、ＡＶデータ転送アプリが正常に稼動する」、「正当な対でないプレーヤ／ビューア間では、ＡＶデータ転送アプリが正常に稼動しない（ビューアでＡＶデータは正常に再生できない）」という状況を実現している。例えば、同一人物が所有する携帯ＭＰＥＧ４プレーヤおよび携帯ビューアを正当な対とした場合に、自分の所有する携帯ＭＰＥＧ４プレーヤからのデータが自分の所有る携帯ビューアで再生されるが、自分の所有する携帯ＭＰＥＧ４プレーヤからのデータが他人の所有る携帯ビューアで再生されず、かつ、自分の所有する携帯ビューアで他人の所有する携帯ＭＰＥＧ４プレーヤからのデータが再生されない、という環境を実現できる。

【００４０】つまり、一般的に、インタフェースが無線の場合には、プレーヤから出力された電波は自ずと一定範囲内のビューアにて受信し得る状態にさらされるので、これをビューア側から見ると、各々の携帯ビューアは、正当な対になる携帯プレーヤにも、それ以外の携帯プレーヤにも、アクセスする（送信を指示する）ことが可能であり得てしまう。ここで、著作権保護レイヤにおいては、両方の装置（送信側の装置と受信側の装置）がＤＴＣＰコンプライアント（ＤＴＣＰ準拠）なデバイスであれば、認証鍵交換は、どちらの場合にも成立し得てしまう。つまり、著作権保護レイヤでは、相手側の装置が正当な対になる装置であるのか、それ以外の装置であ

るのかについて区別することができない。そこで、相手側の装置が正当な対になる装置であるのか、それ以外の装置であるのかを区別するために、本実施形態では、Ｂｌｕｅｔｏｏｔｈレベルの認証を用いるようにしている。

【００４１】すなわち、Ｂｌｕｅｔｏｏｔｈレベルでの認証・鍵交換が成立すると、それは「正当な対になる装置である」と判断し、アプリケーションレベル（ＤＴＣＰレベル）の認証・鍵交換に移行する。Ｂｌｕｅｔｏｏｔｈレベルでの認証・鍵交換が成立しないと、それは「正当な対になる装置ではない」と判断して、アプリケーションレベル（ＤＴＣＰレベル）の認証・鍵交換に移行することを拒否することとする。

【００４２】これは、Ｂｌｕｅｔｏｏｔｈレベルの認証・鍵交換のレベルで認証が成立すれば、その両装置（送信装置と受信装置）が正当な対になる装置であると認識することができることによる。すなわち、Ｂｌｕｅｔｏｏｔｈレベルの認証が、「両装置（送信装置と受信装置）に、同一のＰＩＮコード（例えば、数桁の数字やパスワード、あるいは指紋情報等）を入力することができる」あるいは「両装置（送信装置と受信装置）に、同一のＰＩＮコードが設定されている」ことを根拠として、この値を用いて認証手続きを行なっていることから、この結果、両装置は正当な対であると推測・認識するのに十分である（正当な対でない装置に入力されたＰＩＮコード同士が偶然一致する確立はきわめて小さい）と考えられるためである。

【００４３】例えば、同一人物が所有する（あるいは占有する）携帯ＭＰＥＧ４プレーヤと携帯ビューアが正当な対をなすものとした場合に、Ａ氏が自分の持つ携帯ＭＰＥＧ４プレーヤと携帯ビューアに同一のＰＩＮコード（パスワード）を入力することはできるが、Ｂ氏がこれと同じＰＩＮコード（パスワード）を推測して自分の持つ携帯ビューアに入力することは大変な困難が伴うので、ＭＰＥＧ４プレーヤと携帯ビューアで入力されたＰＩＮコードが同一ならば同一人物が所有する正当な対であると判定し、ＭＰＥＧ４プレーヤと携帯ビューアで入力されたＰＩＮコードが相違するならば異なる人物が所有する正当でない対であると判定することができる。また、ＰＩＮコードに指紋情報等を用いる場合には、Ｂ氏がＡ氏と同じＰＩＮコード（指紋情報等）を自分の持つ携帯ビューアに入力することは、Ａ氏の指紋情報等を盗用でもできないかぎり、不可能である。

【００４４】ここで、図１の携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２との間のやり取りおよび携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０３との間のやり取りを例にとって説明する。

【００４５】図５に、正当な対になるＡ氏の携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２との間で行われるシーケンスの一例を示す。

【００４６】なお、図５においてリンクレイヤによる暗号化および復号化に関する記載は自明であるので省いてある。

【００４７】この場合、まず、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２の両装置には、それぞれ、所定のタイミングで（例えば、事前に、あるいは使用時に）、所定の方法によるＰＩＮコードの入力がなされる（ステップＳ１１，Ｓ１２）。ここでは、携帯ＭＰＥＧ４プレーヤ１０１側で入力されたＰＩＮコードの値をｘとし、携帯ビューア１０２側でもＰＩＮコードの値として同じ値ｘが入力されたものとする。両装置のＰＩＮコードの値が一致することで、続くＢｌｕｅｔｏｏｔｈレイヤ・認証手順を成功裡に終了させることができる。

【００４８】続いて、Ｂｌｕｅｔｏｏｔｈレイヤ・リンクキー共有手順を行って（ステップＳ１３）、それに引き続く認証・鍵交換に用いるリンクキーＫｌの値を共有する（ステップＳ１４，Ｓ１５）。

【００４９】続いて、Ｂｌｕｅｔｏｏｔｈレイヤの認証手順を行う（ステップＳ１６）。この場合は、ＰＩＮコードの共有により、認証が成立する。

【００５０】続いて、Ｂｌｕｅｔｏｏｔｈレイヤ鍵交換手順を行って（ステップＳ１７）、Ｂｌｕｅｔｏｏｔｈレイヤ暗号鍵Ｋｂｔの値を共有する（ステップＳ１８，Ｓ１９）。

【００５１】これによって、Ｂｌｕｅｔｏｏｔｈレイヤにおいて、両装置間で、任意のデータの交換を暗号化の上（他人に盗聴、書き換えができないようにして）行うことができるようになる。

【００５２】次に、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２の両装置は、ＤＴＣＰ（著作権保護レイヤ）の認証・鍵交換を行うフェーズに移る。ここで、両装置は、ＤＴＣＰの認証・鍵交換の手順の全部又は一部を、Ｂｌｕｅｔｏｏｔｈレベルの暗号化を行った上で行うと好ましい。このようにすることで、ＤＴＣＰ認証・鍵交換を、「（Ｂｌｕｅｔｏｏｔｈレベルでの認証・鍵交換に成功した）正当な対をなす装置間でのみ」行なう（完遂する）ことを保証できるようになり、ひいては「正当な対をなす（例えば、同一人物の携帯する）装置間でのみ、著作権保護レイヤ（ＤＴＣＰ）の認証・鍵交換が成立する」、「正当な対をなす（例えば、同一人物の携帯する）装置間でのみ、著作権保護レイヤ（ＤＴＣＰ）レベルの暗号鍵の共有が出来る」ということが可能になる。

【００５３】さて、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０２の両装置は、ＤＴＣＰ認証・鍵交換を、Ｂｌｕｅｔｏｏｔｈレイヤレベルの暗号化を利用して行ない（ステップＳ２０）、両装置間でのＤＴＣＰレイヤ（著作権保護レイヤ）の暗号鍵Ｋｃの共有が達成される（ステップＳ２１，Ｓ２２）。

【００５４】これを受けて、送信側装置である携帯ＭＰ

ＥＧ４プレーヤ１０１は、送信するＡＶコンテンツ（ＭＰＥＧ４データ）を暗号鍵Ｋｃで暗号化して（ステップＳ２３）、受信側装置である携帯ビューア１０２に送信する（ステップＳ２４）。携帯ビューア１０２は、ＤＴＣＰレベルの暗号鍵Ｋｃを共有しているため、この暗号化コンテンツを復号化することが出来、ＭＰＥＧ４データのとりだしを行うことができる。すなわち、携帯ビューア１０２は、受信した暗号化コンテンツをＤＴＣＰレベルの暗号鍵Ｋｃで復号化し（ステップＳ２５）、ディスプレイに表示する。

【００５５】これに対して、同じＢｌｕｅｔｏｏｔｈピコネット内にいる別の受信装置は、ＤＴＣＰレベルの認証・鍵交換を行なっていないため、暗号鍵Ｋｃを共有しておらず、このデータを再生することはできない。これを以下に説明する。

【００５６】図６に、正当な対にならないＡ氏の携帯ＭＰＥＧ４プレーヤ１０１とＢ氏の携帯ビューア１０３との間で行われるシーケンスの一例を示す。

【００５７】まず、携帯ＭＰＥＧ４プレーヤ１０１と携帯ビューア１０３の両装置では、それぞれ、所定のタイミングで（例えば、事前に、あるいは使用時に）、所定の方法によるＰＩＮコードの入力がなされる（ステップＳ３１，Ｓ３２）。

【００５８】しかし、この場合、前述のように携帯ＭＰＥＧ４プレーヤ１０１側で入力されたＰＩＮコードの値をｘとした場合に、携帯ビューア１０３側で入力されたＰＩＮコードの値ｘ’がｘに一致することはないか、または確率的に極めて低い。すなわち、例えば、ＰＩＮコードをユーザが手入力する場合には、両装置は、異なる人物が携帯する装置であるため、両装置に同一のＰＩＮコードが入力されることは非常に難しい。また、正当な対をなす装置に予め固有のＰＩＮコードを書き込んでおく場合には、この例ではＡ氏の携帯ＭＰＥＧ４プレーヤ１０１とＢ氏の携帯ビューア１０３の両装置は正当な対をなす装置ではないものとしているので、両装置のＰＩＮコードが一致することはない。

【００５９】よって、たとえＢｌｕｅｔｏｏｔｈレイヤ・リンクキー共有手順を行って（ステップＳ３３）、それに引き続く認証・鍵交換に用いるリンクキーの値の共有を試みても（ステップＳ３４，Ｓ３５）、ＰＩＮコードが一致していないので、これに基づいて生成された携帯ＭＰＥＧ４プレーヤ１０１側のリンクキーＫｌと、携帯ビューア１０３側のリンクキーＫｌ’とは一致せず、リンクキーの共有は失敗に終わることになる。

【００６０】従って、続くＢｌｕｅｔｏｏｔｈレイヤ認証手順を行っても（ステップＳ３６）、これは失敗に終わることになる。この結果、これに引き続くＢｌｕｅｔｏｏｔｈレイヤ鍵交換手順が行なわれない。

【００６１】そして、Ｂｌｕｅｔｏｏｔｈ暗号化が成立しないため、ＤＴＣＰ認証・鍵交換手順に入ることができず、ＤＴＣＰの認証・鍵交換を成功裡に行うことができない。すなわち、送信側の携帯ＭＰＥＧ４プレーヤ１０１は、もし、受信側の携帯ビューア１０３より、ＤＴＣＰレベルの認証・鍵交換の要求が来たとしても（ステップＳ３７）、これがＢｌｕｅｔｏｏｔｈレベルの暗号化がなされない形で送信されてきた場合には、これを拒否する（ステップＳ３８）。よって、正当な対でない（例えば、所有者が異なる）装置同士では、著作権保護レベルの認証・鍵交換が成立せず、著作権を保護すべきＡＶデータの転送は、行なえないこととなる。

【００６２】なお、ステップＳ３８の拒否メッセージを相手に通知する際に、その拒否の理由（リンクレイヤすなわちＢｌｕｅｔｏｏｔｈレイヤの暗号化がかかっていないため、あるいはＢｌｕｅｔｏｏｔｈレイヤの認証が行われていないため）を併せて通知するようにしてもよい。これは、相手が正当なもの（例えば同一所有者のもの）である場合に、Ｂｌｕｅｔｏｏｔｈレイヤの認証・鍵交換の実行を促すものとなる。

【００６３】なお、以上では、携帯ＭＰＥＧ４プレーヤにＭＰＥＧ４データが蓄積されているものとしているが、ＭＰＥＧ４データを外部から取得するものであってもよいし、符号化する前のソースデータが蓄積されていてＭＰＥＧ４コーダを備えてＭＰＥＧ４を生成してもよいし、ソースデータを外部から取得しＭＰＥＧ４コーダでＭＰＥＧ４を生成してもよい。また、ＭＰＥＧ４映像（ＭＰＥＧ４データ）以外のデータの送受信にも本発明はもちろん適用可能である。

【００６４】また、以上では、送信装置１台に対して受信装置を１台とする通信を前提として説明したが、送信装置から複数台の受信装置へのデータ転送も可能である。この場合には、例えば、図５のシーケンスにおいて、携帯ＭＰＥＧ４プレーヤと各々の携帯ビューアとの間で、暗号鍵Ｋｃの共有までの手順を、逐次行って、認証・鍵交換に成功した全装置で暗号鍵Ｋｃを共有するようにしてもよい。この結果、携帯ＭＰＥＧ４プレーヤがＡＶコンテンツを暗号鍵Ｋｃで暗号化して送信すれば、暗号鍵Ｋｃの共有に成功した正当な携帯ビューアは、暗号化コンテンツを復号化し、表示することができる。なお、この場合に、送信装置ごとに、あるいはコンテンツごとに、送信装置から同時にデータ転送可能な受信装置の台数の上限を設定可能にしてもよい。

【００６５】（第２の実施形態）第１の実施形態では、著作権保護レイヤ（ＤＴＣＰ）の認証・鍵交換の手順の全部又は一部を、Ｂｌｕｅｔｏｏｔｈレイヤの暗号・復号化部を通して行うものであった。これに対して、第２の実施形態は、ＭＰＥＧ４データ（ＡＶデータ）の転送そのものについても、Ｂｌｕｅｔｏｏｔｈレイヤの暗号・復号化部を通して行うようにしたものである。

【００６６】本実施形態では、第１の実施形態と相違する部分を中心に説明する。

【００６７】図７に、第１の実施形態における図２に対応する本実施形態の携帯ＭＰＥＧ４プレーヤ１０１の内部構造の一例を示す。また、図８に、第１の実施形態における図３に対応する本実施形態の携帯ビューア１０２（１０３）の内部構造の一例を示す。いずれも、第１の実施形態に対して、ＢＴレイヤ暗号・復号化部がｂｌｕｅｔｏｏｔｈ通信処理部とＤＴＣＰ暗号化部との間に接続されている点が相違する。

【００６８】また、図９に、第１の実施形態における図５のシーケンス例に対応する本実施形態におけるシーケンスの一例を示す。

【００６９】なお、図９においてリンクレイヤによる暗号化および復号化に関する記載は自明であるので省いてある。

【００７０】これは、第１の実施形態に対して、ＡＶデータが、ＤＴＣＰレイヤ（著作権保護レイヤ）の暗号鍵ＫｃとＢｌｕｅｔｏｏｔｈレイヤ暗号鍵Ｋｂｔによって多重に暗号化されている点が相違する。すなわち、携帯ＭＰＥＧ４プレーヤは、送信する著作権保護すべきＡＶコンテンツを暗号鍵Ｋｃで暗号化した後に、暗号鍵Ｋｂｔで暗号化する。また、携帯ビューア１０２は、受信した暗号化されたＡＶコンテンツを暗号鍵Ｋｂｔで復号化した後に、暗号鍵Ｋｃで復号化する。

【００７１】本実施形態は、第１の実施形態と比べ、ＤＴＣＰの認証・鍵交換手順及びデータ暗号化・復号化の両方について、Ｂｌｕｅｔｏｏｔｈ暗号化をかけて行うため、処理速度は遅くなるものの、装置構成は単純なものにすることが可能となる（例えば、ＤＴＣＰ処理を単一のＬＳＩで行なっている場合には、全ての入出力を、Ｂｌｕｅｔｏｏｔｈレイヤ暗号・復号化部を経由させることで、構成が単純になる）。

【００７２】なお、本実施形態においても、正当な対でない（例えば、異なる人物の）装置間では、両装置に同一のＰＩＮコードが入力されることは非常に難しいため、Ｂｌｕｅｔｏｏｔｈレイヤ認証手順が失敗してしまう。よって、これに引き続くＢｌｕｅｔｏｏｔｈレイヤ鍵交換手順が行なわれない。よって、この後、Ｂｌｕｅｔｏｏｔｈ暗号化が成立しないため、ＤＴＣＰ認証・鍵交換手順に入ることができず、ＤＴＣＰの認証・鍵交換を成功裡に行うことができない。よって、正当な対でない（例えば、所有者が異なる）装置同士では、著作権を保護すべきＡＶデータの転送は、第１の実施形態と同じく、行なえないこととなる。

【００７３】なお、本実施形態では、無線ＬＡＮとして、Ｂｌｕｅｔｏｏｔｈを例に説明してきたが、８０２．１１無線ＬＡＮや、ＷＥＣＡ方式、ＨｏｍｅＲＦ方式の無線ＬＡＮ等、リンクレイヤレベルで認証・鍵交換、暗号化等のセキュリティ機能を持つ無線ＬＡＮは多い。本発明は、これらの種々の無線ＬＡＮに適用することが可能である。

【００７４】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【００７５】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【００７６】なお、各実施形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。また、各実施形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

【００７７】従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【００７８】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００７９】

【発明の効果】本発明では、認証手続きを成功させることのできる正当な装置間でのみ、正しく暗号鍵を共有することができ、正しく暗号鍵を共有することができた装置間でのみ、暗号通信によるデータ転送が可能になる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る無線通信システムの構成例を示す図

【図２】同実施形態に係る携帯ＭＰＥＧ４プレーヤの内部構造の一例を示す図

【図３】同実施形態に係る携帯ビューアの内部構造の一例を示す図

【図４】Ｂｌｕｅｔｏｏｔｈレイヤの認証手順の概要を説明するためのフローチャート

【図５】正当な対になる携帯ＭＰＥＧ４プレーヤと携帯ビューアとの間で行われるシーケンスの一例を示す図

【図６】正当な対にならない携帯ＭＰＥＧ４プレーヤと

19　　20

携帯ビューアとの間で行われるシーケンスの一例を示す図

【図７】同実施形態に係る携帯ＭＰＥＧ４プレーヤの内部構造の他の例を示す図

【図８】同実施形態に係る携帯ビューアの内部構造の他の例を示す図

【図９】正当な対になる携帯ＭＰＥＧ４プレーヤと携帯ビューアとの間で行われるシーケンスの他の例を示す図

【符号の説明】

１１，２１…Ｂｌｕｅｔｏｏｔｈインタフェース処理部

１２，２２…ｂｌｕｅｔｏｏｔｈ通信処理部

１３，２３…ＢＴ認証・鍵交換処理部

＊１４，２４…ＰＩＮコード入力部

１５，２５…ＢＴレイヤ暗号・復号化部

１６，２６…ＤＴＣＰ認証・鍵交換部

１７…ＤＴＣＰ暗号化部

１８…パケット化部

１９…ＭＰＥＧ４ストレージ

２７…ＤＴＣＰ復号化部

２８…パケットリアセンブリ部

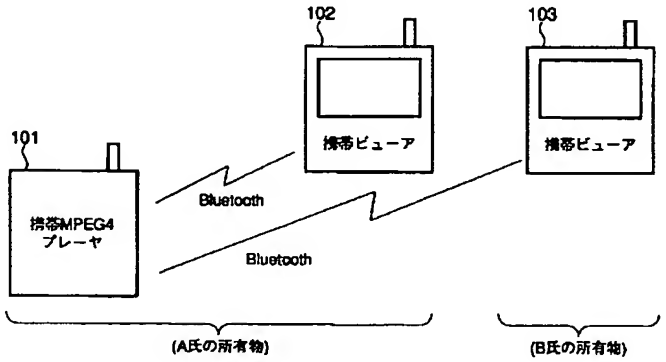
２９…ＭＰＥＧ４デコーダ

３０…ディスプレイ

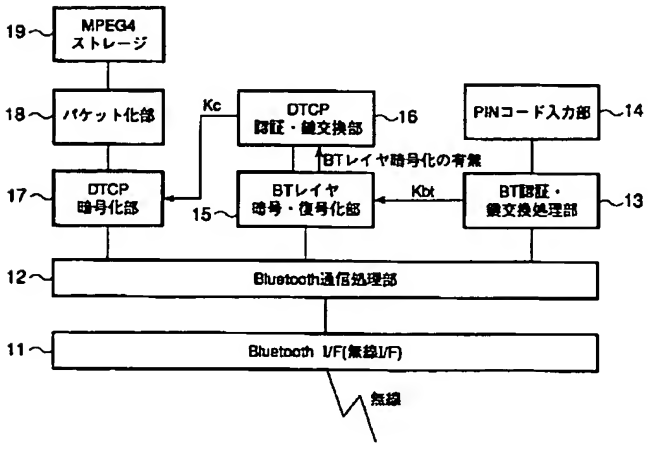
１０１…ＭＰＥＧ４プレーヤ

１０２，１０３…携帯ビューア

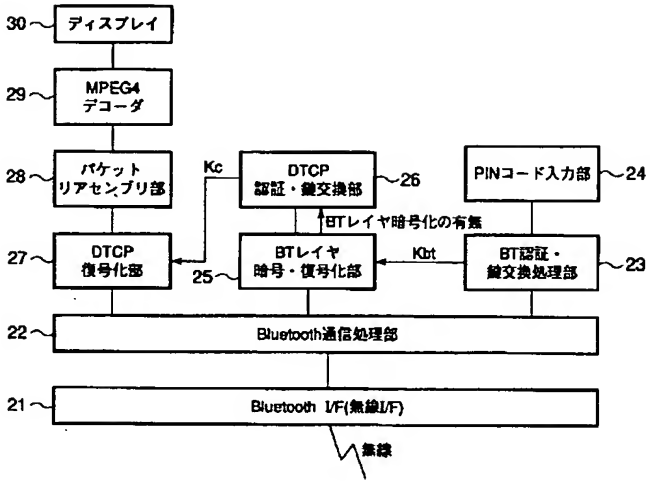
【図１】



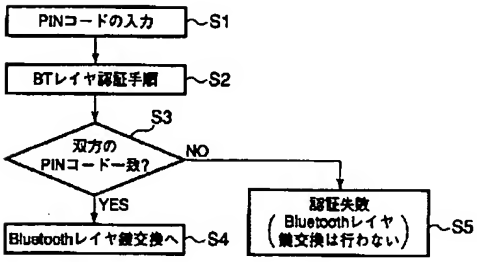
【図２】



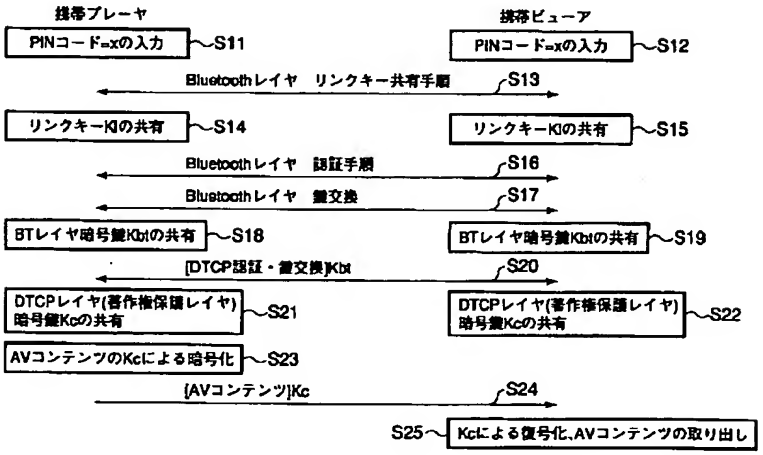
【図３】


30
ディスプレイ
29
MPEG4
デコーダ
28
パケット
リアセンブリ部
Kc
DTCP
認証・鍵交換部
26
PINコード入力部
24
BTレイヤ暗号化の有無
27
DTCP
復号化部
25
BTレイヤ
暗号・復号化部
Kbt
BT認証・
鍵交換処理部
23
22
Bluetooth通信処理部
21
Bluetooth I/F(無線I/F)
無線

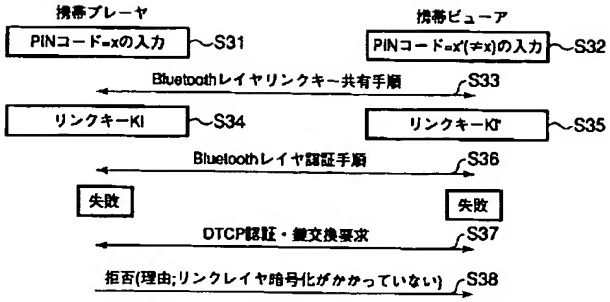
【図４】


PINコードの入力
S1
BTレイヤ認証手順
S2
S3
双方の
PINコード一致?
NO
YES
Bluetoothレイヤ鍵交換へ
S4
認証失効
(Bluetoothレイヤ
鍵交換は行わない)
S5

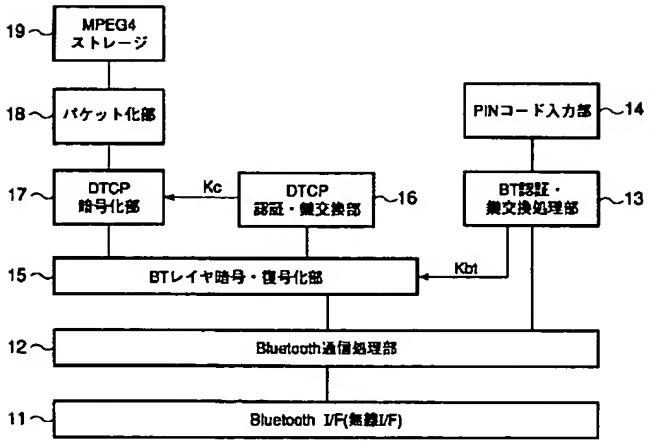
【図５】


携帯プレーヤ
携帯ビューア
PINコード=xの入力
S11
PINコード=xの入力
S12
Bluetoothレイヤ リンクキー共有手順
S13
リンクキーKlの共有
S14
リンクキーKlの共有
S15
Bluetoothレイヤ 認証手順
S16
Bluetoothレイヤ 鍵交換
S17
BTレイヤ暗号鍵Kbtの共有
S18
BTレイヤ暗号鍵Kbtの共有
S19
[DTCP認証・鍵交換]Kbt
S20
DTCPレイヤ(著作権保護レイヤ)
暗号鍵Kcの共有
S21
DTCPレイヤ(著作権保護レイヤ)
暗号鍵Kcの共有
S22
AVコンテンツのKcによる暗号化
S23
[AVコンテンツ]Kc
S24
S25
Kcによる復号化、AVコンテンツの取り出し

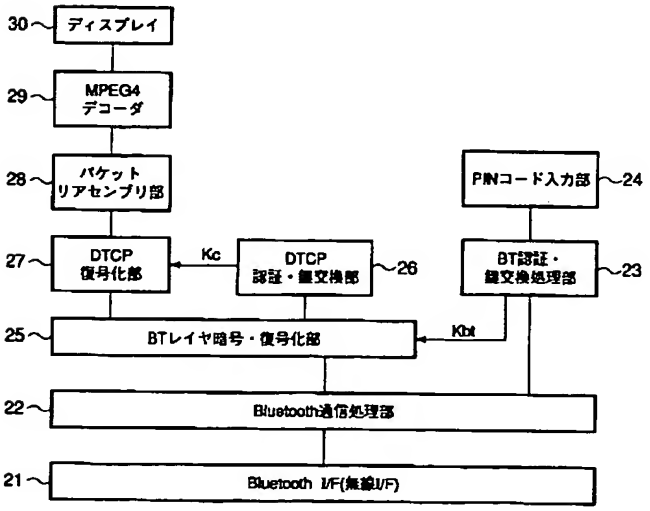
【図６】


携帯プレーヤ
携帯ビューア
PINコード=xの入力
S31
PINコード=x'(≠x)の入力
S32
Bluetoothレイヤリンクキー共有手順
S33
リンクキーKl
S34
リンクキーKl'
S35
Bluetoothレイヤ認証手順
S36
失敗
失敗
DTCP認証・鍵交換要求
S37
拒否(理由;リンクレイヤ暗号化がかかっていない)
S38

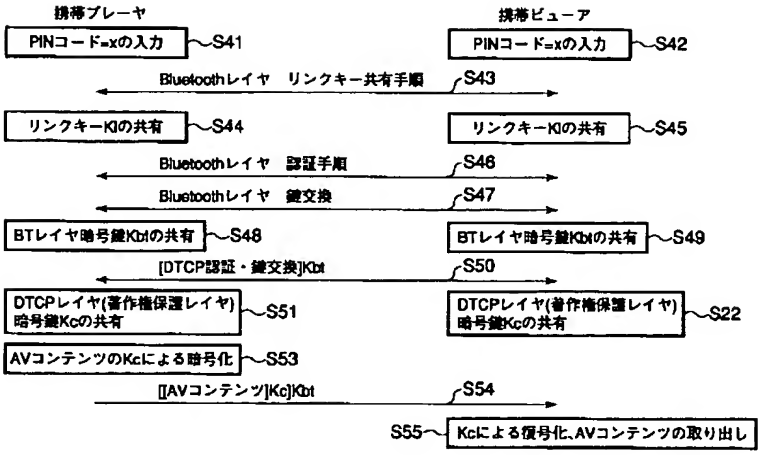
【図７】


19
MPEG4 ストレージ
18
パケット化部
PINコード入力部
14
17
DTCP 暗号化部
Kc
DTCP 認証・鍵交換部
16
BT認証・ 鍵交換処理部
13
15
BTレイヤ暗号・復号化部
Kbt
12
Bluetooth通信処理部
11
Bluetooth I/F(無線I/F)

【図８】


30
ディスプレイ
29
MPEG4 デコーダ
28
パケット リアセンブリ部
PINコード入力部
24
27
DTCP 復号化部
Kc
DTCP 認証・鍵交換部
26
BT認証・ 鍵交換処理部
23
25
BTレイヤ暗号・復号化部
Kbt
22
Bluetooth通信処理部
21
Bluetooth I/F(無線I/F)

【図９】



フロントページの続き

(51)Int.Cl.'		識別記号	F I		テーマコード(参考)
Ｇ１０Ｌ	19/00		Ｈ０４Ｌ 12/28		３００Ｚ
Ｈ０４Ｑ	7/38		Ｇ１０Ｌ 9/00		Ｎ
Ｈ０４Ｌ	9/32		Ｈ０４Ｂ 7/26		１０９Ｒ
	12/28	３００	Ｈ０４Ｌ 9/00		６７３Ｄ
					６７５Ａ

Ｆターム(参考) 5B085 AA08 AE01 AE04 AE25 AE29
5J104 AA01 AA07 AA15 JA03 KA01
KA04 KA16 KA17 NA02 NA05
5K033 AA08 BA13 BA15 CB14 CC01
DA19
5K067 AA32 BB21 DD17 EE02 HH12
HH24 HH36

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年10月20日(2005.10.20)

【公開番号】特開2002-140304(P2002-140304A)
【公開日】平成14年5月17日(2002.5.17)
【出願番号】特願2001-28544(P2001-28544)
【国際特許分類第７版】
Ｇ０６Ｆ　15/00
Ｇ０６Ｆ　17/60
Ｇ１０Ｋ　15/02
Ｇ１０Ｌ　19/00
Ｈ０４Ｑ　 7/38
Ｈ０４Ｌ　 9/32
Ｈ０４Ｌ　12/28
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ｃ
Ｇ０６Ｆ　15/00　３３０Ｂ
Ｇ０６Ｆ　15/00　３３０Ｆ
Ｇ０６Ｆ　17/60　３０２Ｅ
Ｇ１０Ｋ　15/02
Ｈ０４Ｌ　12/28　３００Ｚ
Ｇ１０Ｌ　 9/00　　Ｎ
Ｈ０４Ｂ　 7/26　１０９Ｒ
Ｈ０４Ｌ　 9/00　６７３Ｄ
Ｈ０４Ｌ　 9/00　６７５Ａ

【手続補正書】
【提出日】平成17年6月30日(2005.6.30)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、
前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第１の認証手段と、
この第１の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、
前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、
この第２の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項２】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおいて、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置と前記受信装置との間で認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置と前記受信装置との間で著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とする無線通信システム。

【請求項３】

著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記受信装置へ前記コンテンツデータを送信することを特徴とする無線通信システム。

【請求項４】

著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、

前記受信装置が前記送信装置と通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記受信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記受信装置との間で認証が成功した場合、前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記受信装置との間で著作権保護のための認証が成功した

場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。

【請求項５】

前記第２の認証手段または前記第２の鍵交換手続き手段は、前記無線リンクレイヤ上における暗号化通信が介在しなかったことを理由として、前記著作権保護のための認証または前記第２の暗号鍵の共有が失敗した場合に、該失敗の旨および該理由を前記受信装置に通知することを特徴とする請求項３または４に記載の送信装置。

【請求項６】

前記コンテンツ・データを記憶するための記憶手段を更に備えたことを特徴とする請求項３ないし５のいずれか１項に記載の送信装置。

【請求項７】

前記第１の認証手段による前記認証は、自装置に入力されたＰＩＮコードと前記受信装置から通知されたＰＩＮコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項３ないし６のいずれか１項に記載の送信装置。

【請求項８】

前記ＰＩＮコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項３ないし７のいずれか１項に記載の送信装置。

【請求項９】

著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項１０】

著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、

自装置が前記送信装置と通信することを許可された機器として動作可能とするために、前記無線通信の無線リンクレイヤ上にて、前記送信装置との間の認証を行う第１の認証手段と、

この第１の認証手段により、前記送信装置との間で認証が成功した場合、前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する第１の鍵交換手続き手段と、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う第２の認証手段と、

この第２の認証手段により、前記送信装置との間で著作権保護のための認証が成功した

場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する第２の鍵交換手続き手段とを備え、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。

【請求項１１】

前記コンテンツ・データを表示するための表示手段を更に備えたことを特徴とする請求項９または１０に記載の受信装置。

【請求項１２】

前記第１の認証手段による前記認証は、自装置に入力されたＰＩＮコードと前記送信装置から通知されたＰＩＮコードとが予め定められた一定の関係にある場合に、成立するものであることを特徴とする請求項９ないし１１のいずれか１項に記載の受信装置。

【請求項１３】

前記ＰＩＮコードは、その都度変化するコード情報、予め定められたコード情報、ユーザの身体から採取した身体情報、またはユーザの属性に関する属性情報の少なくとも一つを含むものであることを特徴とする請求項９ないし１２のいずれか１項に記載の受信装置。

【請求項１４】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有し、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有し、

前記無線リンクレイヤ上に設けられた、前記第２の暗号鍵に基づき暗号化された暗号化通信路を用いて前記送信装置から前記受信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。

【請求項１５】

無線通信を介して著作権を保護すべきコンテンツデータを送信する送信装置と、この送信装置から送信された前記コンテンツデータを受信する受信装置からなる無線通信システムにおけるコンテンツデータ転送方法であって、

前記受信装置と前記送信装置とが互いに通信することを許可された機器であるか否かを判断するために、前記無線通信の無線リンクレイヤ上にて、前記送信装置と前記受信装置との間の認証を行い、

この前記送信装置と前記受信装置との間での認証が成功した場合、前記送信装置と前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有し、

前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置と前記受信装置との間で、著作権保護のための認証を行い、

この前記送信装置と前記受信装置との間での著作権保護のための認証が成功した場合、前記送信装置と前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有し、

前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から前記受

信装置へ前記コンテンツデータを転送することを特徴とするコンテンツデータ転送方法。
【請求項１６】
著作権を保護すべきコンテンツデータを無線通信を介して受信装置へ送信する送信装置であって、
前記受信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する手続を行う第１の鍵交換手続き手段と、
前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記受信装置との間で、著作権保護のための認証を行う認証手段と、
この認証手段により、前記受信装置との間で著作権保護のための認証が成功した場合、前記受信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する手続を行う第２の鍵交換手続き手段とを備え、
前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記受信装置へ前記コンテンツデータを転送することを特徴とする送信装置。
【請求項１７】
著作権を保護すべきコンテンツデータを送信する送信装置から無線通信を介して送信された前記コンテンツデータを受信する受信装置であって、
前記送信装置との間で共通の第１の暗号鍵を生成し、この第１の暗号鍵を共有する手続を行う第１の鍵交換手続き手段と、
前記第１の暗号鍵に基づき暗号化された無線通信を用いて、前記送信装置との間で、著作権保護のための認証を行う認証手段と、
この認証手段により、前記送信装置との間で著作権保護のための認証が成功した場合、前記送信装置との間で共通の第２の暗号鍵を生成し、この第２の暗号鍵を共有する手続を行う第２の鍵交換手続き手段とを備え、
前記第２の暗号鍵に基づき暗号化された暗号化通信路を、前記第１の暗号鍵に基づき暗号化された前記無線通信上に設定し、この暗号化通信路を介して前記送信装置から送信された前記コンテンツデータを受信することを特徴とする受信装置。